ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

April 12, 2021

Via eRulemaking Portal

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E–218
Washington, DC 20219

Ann Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

James Sheesley, Assistant
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Re: Comments Regarding the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers – Docket ID OCC–2020–0038 and RIN 1557–AF02; FRB Docket No. R–1736 and RIN 7100–AG06; FDIC RIN 3064–AF59

To whom it may concern:

On behalf of the Electronic Transactions Association ("ETA"), we appreciate the opportunity to share our thoughts on the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation ("Agencies") noticed of proposed rulemaking relating to computer-security incident notification requirements for banking organizations and their bank service providers.

ETA members support the Agencies' goal of ensuring timely awareness of significant cybersecurity threats in order to promote the safety and soundness of the financial system. In that regard, we appreciate the Agencies' effort to reduce additional burden to maximize the bank service providers and financial institution's ability to protect consumers and restore the confidence in the systems that the ecosystem relies on. However, there are a number of concerns and these recommendations are intended to bring additional clarity and consistency to the proposed incident reporting framework, to ensure the Agencies receive timely notification of the significant cybersecurity incidents that are the focus of the proposed rule, and to minimize excess burden on bank service providers and financial institutions, including by avoiding unnecessary and burdensome over-reporting of less significant or easily remediated matters not intended to be captured by the proposed rule.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Who We Are

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include banks, mobile payment service providers, mobile wallet providers, money transmitters and non-bank financial technology companies ("FinTech") that provide access to credit, primarily to small businesses, either directly or in partnership with other lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient, and rewarding payment solutions and lending alternatives – facilitating over $22 trillion in payments in 2019 worldwide.

Comments

36-Hour Timeframe for Notification

ETA members appreciate the importance of early detection of significant cybersecurity incidents and support the goal of ensuring early detection of emerging threats to individual banking organizations and the broader financial system. We also appreciate the Agencies' acknowledgment that, in requiring bank service providers and financial institutions to provide notification "as soon as possible and no later than 36 hours" after they believe in good faith that a notification incident has occurred. We believe a 36-hour notification timeframe should be modified to require notification as soon as "practicable" and no later than 72 hours after a notification incident has occurred. This would align the proposed rule with New York's Department of Financial Services Cybersecurity Regulation and allow the proper gathering of available information at a point in time to develop and send communication.

In addition, to eliminate the burden of over-reporting that fall below the reporting threshold after appropriate review or investigation is performed, we believe it is critical that bank service providers and financial institutions understand that they can conduct such review or investigation, consistent with the proposed rule's reporting requirements, before determining that a notification incident has occurred.

Harmonizing Incident Definitions

The proposed rule defines "computer-security incident" as "an occurrence that: (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or (ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." The proposed rule defines "notification incident" as "a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair: (i) the ability of the banking organization to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or (iii) those operations of a banking organization, including associated services,

functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States."

We acknowledge and support the Agencies policy goals of minimizing compliance burden for bank service providers and financial institutions and should use "notification incident" as the primary incident reporting threshold.

This would reduce the number of high volume and less significant or easily remediated occurrences and incidents that do not result in actual harm should not give rise to a notification incident given the stated objectives of the proposed rule.

By adopting the "notification incident" definition, bank service providers and financial institutions would not have to report occurrences of no consequences that happen daily, such as phishing emails. The inclusion of these less significant occurrences would place unnecessary burden on bank service providers and financial institutions and the unintended result would be over-reporting to the Agencies.

Notifying the Agencies

We agree with the Agencies' decision to allow notification through any technological means, but believe it is also critical to provide multiple potential channels of communication of notification incidents. During a disruptive incident, some channels of communication may not be operational or secure. Additionally, a bank service provider or financial institution may determine that it has experienced a notification incident during a holiday, at the start of a weekend, or at other times during which any particular method may be less desirable or any designated agency representative may be unavailable. Permitting notification to any of several points of contact and through multiple channels would help ensure that the Agencies receive the notification timely.

We believe that simplicity of the notification is critical to the effectiveness of the proposed rule, and that requiring any specific information or assessment would result in a complex, uncertain, and burdensome process at a sensitive time. Additionally, any requirements for information that need to be included in the notification should be standardized and clearly identified to help ensure bank service providers and financial institutions are communicating the expected information, if available, in order to minimize repeated follow-up questions from the Agencies.

Given the critical need of being a time sensitive manner, we recommend allowing "significant service providers" to directly alert the Agencies of an incident. The Agencies currently have statutory authority to supervise third-party servicers that enter into contractual arrangements with their regulated financial institutions. With this explicit consent, it would minimize the burden these organizations in post-notification communications while the notification incident is ongoing. We recommend that the final rule require bank service providers to notify their banking organization in a reasonable manner, after a relevant incident.

We also welcome further discussion about how the Agencies intend to share and secure any information provided by an organization in connection with a notification incident, an issue of critical importance to our members. For example, will or under what circumstances the Agencies

share the information with other authorities and how the Agencies would ensure the reporting data is safe and secure.

* * *

ETA appreciates the opportunity to provide input on this important issue. If you have any questions, please contact myself or ETA's Senior Vice President of Government Affairs, Scott Talbott at stalbott@electran.org.

Sincerely,

Jeff Patchen
Manager of Government Affairs
Electronic Transactions Association
jpatchen@electran.org
(202) 677-7418